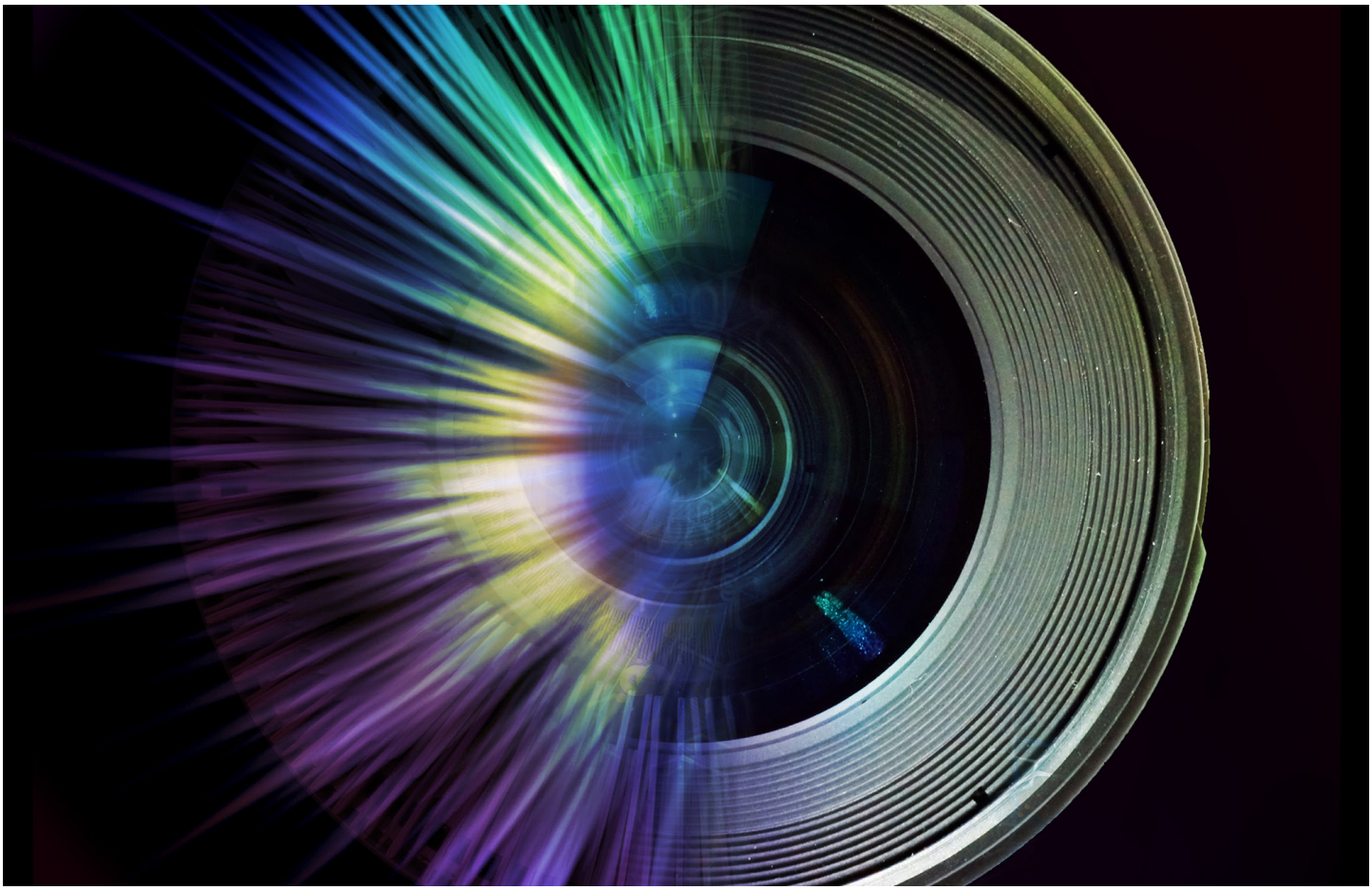
Deloitte.



Forensic Focus on COVID-19

Opportunities to enhance compliance programs while working remotely and with reduced budgets

This is the ninth in a Deloitte Forensic series around COVID-19 business impacts and steps you can proactively take to help respond to and recover from the outbreak and mitigate potential fraud and financial crime risks.

Companies continue to face significant financial, operational, and strategic challenges as a result of the novel coronavirus (COVID-19) pandemic, and such challenges are likely to persist at least for the near term.

Compliance teams in particular face specific challenges on each of these fronts. From a financial perspective, many companies will be tightening their belts, reducing compliance budgets, reallocating resources to meet current and near-term needs, and otherwise weathering the slowdown. From an operational standpoint, compliance reviews and assessments will largely have to be performed remotely, with international travel, site visits, live interviews, gathering hard-copy documents, and other typical steps on hold.

The new environment posed by the pandemic may create heightened and/or different risks.

And in terms of strategic challenges, companies may be hesitant to introduce overall structural changes to the compliance framework during this period of great uncertainty, where other dramatic changes may be more mission-critical. Moreover, with supply chain interruptions and other emergent needs, companies may feel the pressure to simplify or avoid typical procedures that may otherwise take days or weeks—such as onboarding new vendors and business partners.

Nevertheless, even working from home and with significantly reduced budgets, there are still meaningful opportunities to assess and improve corporate compliance programs:

- **Identify emerging risks and other significant near-term changes to your risk profile and adjust accordingly**. The new environment posed by the pandemic may create heightened and/or different risks:
  - Elevated fraud risk might be particularly steep. In a downturn, there may be pressure to perform (or at least report a certain measure of performance) at all levels—whether the entire company, individual business units, subsidiaries, and/or individuals. Fraudsters may also look to take advantage of weakened first- and second-line internal controls caused by increased remote work (that is, less "over-the-shoulder" review). Your business partners and other third parties might also be feeling economic pressure. All of these might lead to shortcuts, risky behavior, or outright fraudulent and deceptive practices. On the flip side, reduced headcount and/or remote personnel may affect your control environment.
  - Due to supply chain interruption or other crises, you might have an urgent, time-sensitive need to plug the hole by engaging new third parties. There might be pressure to expedite standard controls and procedures (e.g., due diligence) typically taken in order to quickly onboard new vendors and other third parties.
  - With employees working remotely and perhaps accessing sensitive data at home for the first time, you might have an emerging cyber risk.
  - The list goes on.

From our experience, a number of companies have found themselves subject to regulatory scrutiny when compliance changes lag behind a change in that company's risk profile. So even if you are not scheduled to conduct your company's periodic risk assessment in the near term, it might be worthwhile to assess whether your risk profile might have changed significantly as a result of the pandemic. Set up video calls with your business leaders and other compliance champions, and speak to them about what they are seeing from an emerging risk perspective. Examine the impact of the current situation and look for changes in your business or business practices that might create additional risk. Then, once that risk is identified, consider what compliance adjustments can be made in the short term and longer term to mitigate those risks.

- **Get current on the latest guidance and identify areas for potential improvement**. When stuck at home, it doesn't cost anything to take stock (or restock) of the latest guidance. Even if you reviewed them when they were first issued, it might help to take a fresh look at the most recent formal guidance (such as the Department of Justice's (DOJ) April 2019 Evaluation of Corporate Compliance Programs[1] or the ISO 37001 standards[2]). You can get a good sense of the importance the DOJ places on certain aspects of its guidance based on where it's placed and how often it's emphasized.

  But don't limit yourself to formal guidance. Take this time to review major enforcement actions and legal commentary on those actions, where descriptions of corporate compliance weaknesses and failures, as well as root cause discussions, can reveal insights about the compliance emphases of the DOJ, SEC, and foreign regulators. Ask yourself if a regulator, taking perhaps a more jaundiced perspective of your program after a compliance breakdown, could make analogous assertions about your program.

Once you've reviewed the available guidance, make an honest assessment of whether there are opportunities for enhancement or areas for potential refocus. For example, consider:

- Have you assessed the "effectiveness of [your] company's risk assessment and the manner in which the company's compliance program has been *tailored* based on that risk assessment"?[3] Can the regulators contend that the company "devote[d] a disproportionate amount of time to policing low[er]-risk areas instead of high[er]-risk areas"?[4]
- Is your training program truly meeting the revised guidance? In other words, is there "appropriately tailored" and effectiveness-assessed training whereby gatekeepers, high-risk employees, and supervisors receive "different or supplementary training" as more fully described in the guidance?[5] How should such programs evolve in the absence of in-person training options?
- Is there a credible system for disciplining "responsible" employees, including supervisors? Current DOJ guidance makes clear its position that discipline is appropriate not just for "those identified by the company as responsible for the misconduct . . . through direct participation," but also for those who bear responsibility for "failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred."[6]
- For internal investigations, are you "apply[ing] timing metrics to ensure responsiveness" and utilizing a process for ensuring confirming accountability for the response to any findings or recommendations?"[7]
- How's both your tone and demonstrated conduct at the top? Can you, in a nonanecdotal way, demonstrate that your leaders—both senior leaders and middle-management—have taken "concrete actions" and "modelled proper behavior" to reinforce compliance and remediation efforts?[8]

- **Amend investigative strategies to adapt to current environment**. While companies might choose to delay or truncate some categories of investigations and other compliance matters, others will inevitably require fuller and more immediate attention, whether because of their severity, potential implications, reporting obligations, or otherwise. However, the current environment makes "traditional" investigative techniques such as travel for site visits, in-person interviews, and physical discovery significantly more challenging. As such, companies will need to adapt their investigative strategies so that they can productively and proactively investigate potential misconduct. In that respect, there are numerous technology-driven platforms available to help perform data and information collection and analysis, as well as provide virtual connectivity for interviews and investigation needs. Questions companies may want to ask include:
  - In the absence of being able to travel to the location for a site visit, what remote capabilities do we have to collect key information (including images of desktops and mobile devices) in a secure way?
  - What's the appropriate method for remotely sharing and analyzing large volumes of unstructured (such as email) and/or structured (such as accounting) data?
  - What's the optimal approach for conducting interviews? Which ones can be done remotely via video conference, and which ones are so critical that (subject to any travel restrictions) an in-person meeting is necessary?

As companies continue to evaluate their business operations in the wake of the COVID-19 outbreak, they may want to consider how to efficiently and effectively prioritize their investigations portfolio and implement remote, digital technologies. Please see our colleagues' article on conducting effective remote investigations for further suggestions.[9]

- **Test what you can test**. Despite travel and budgetary restrictions, there are meaningful assessments you can conduct regarding the effectiveness of your compliance program. For example:
  - Third-party approval procedures. Select, collect, review, and assess a sample of your high-risk third-party approval packages.
    - Did the person reviewing the due diligence report and other preapproval materials (such as questionnaires) correctly identify all red flags, require appropriate risk mitigation, and come to the proper conclusion?
    - Was any required risk mitigation appropriately implemented?
    - Were all appropriate contractual provisions put into the contract?
  - Third-party monitoring. For your high- and highest-risk third parties:
    - Did the third party meet all of its compliance obligations under the contract (for example, adoption of policies and procedures, periodic certifications or representations, or annual training)?
    - Was the third party's compliance with its obligations under the contract previously reviewed and assessed by the appropriate stakeholder (whether at a periodic assessment, upon renewal of the third party's agreement, or at some other appropriate interval)?
    - Was the third party subject to an audit? If so, were the results properly assessed and any identified risks appropriately mitigated? If not subject to an audit, should they have been? Are any changes to the company's risk-based third-party audit plan appropriate?
  - Third-party payment procedures. Select a sample of your highest-risk third-party payments and review whether gatekeepers served as a meaningful check on potentially suspicious or inappropriate payments.
    - Were appropriate procedures followed?
    - Was there appropriate supporting documentation available (such as invoice or proof of performance) to substantiate the nature and amount of the payment?
    - Did finance correctly identify red flags and, as appropriate, either investigate or elevate prior to approval?
  - Hotline responses. Select a sample of compliance-related hotline calls and whistleblower complaints.
    - Were the calls or complaints triaged and elevated properly? Investigated thoroughly and in a timely matter?
    - Did the whistleblower face any retaliation or perceived retaliation? If so, was that addressed fully and effectively?
    - Was there a proper and thorough root cause analysis and remediation plan, including appropriate discipline and messaging consistent with DOJ guidance?
  - Follow up on remediation plans. Many compliance teams spend much of their time putting out fires. When the next fire hits, it's very easy to lose track of the prior fires that appear to be extinguished—it's the reality of overburdened compliance teams who might be in constant triage mode. More specifically, one of the more serious compliance failures we've observed (on many occasions) is when companies investigate properly, develop a thoughtful remediation plan, but lack follow-through (for a variety of reasons), and at some later period, similar or even the same misconduct is occurring and the remediation that was supposed to be implemented is no longer operating effectively (again, for a variety of reasons). Having a remediation plan with recommendations that are not being followed can substantially undermine efforts to demonstrate to regulators an earnest commitment to and culture of compliance.

So, use this time to review the most recent remediation plans resulting from significant investigations, and determine:

- Were required remedial actions fully implemented by the assigned stakeholder within the deadlines set?
- Have those implemented remedial actions been assessed for effectiveness?
- Has there been any slippage or backsliding? Has a terminated third party been rehired? Is finance currently reviewing payments for the types of red flags that they may have missed in the prior investigation?

- **Brainstorm those pesky strategic transformations**. In fact, the limitations imposed during this shutdown might afford compliance officers the opportunity to begin to tackle the larger transformational changes that might be needed.
  - Centralized versus decentralized compliance. For those companies with a more centralized compliance program and fewer local compliance resources, the inability to travel might lead to less oversight and an increase in compliance blind spots, which could result in increased risks. Even with a more decentralized program, the inability to travel and conduct site visits might make it more difficult to confirm consistency across regions, leading to different risks.
  - Despite regulatory guidance emphasizing the importance of postcontractual monitoring and the exercising of audit rights for a company's highest-risk third parties, many companies continue to shy away from a more robust implementation of such guidance, to avoid threatening relationships with critical third parties.
  - Improved buy-in by business leaders. One of the more effective changes we've seen in terms of obtaining compliance buy-in from reluctant business leaders is to make compliance part of their performance metrics. We've heard compliance officers state that nothing was more effective in increasing the participation rate for mandatory training than making 100 percent compliance a metric in middle management's bonuses. Similarly, when the true costs of compliance—such as third-party preapproval procedures or the costs of internal investigations—do not hit compliance's cost center, but are reflected in the respective business unit's bottom line, those business leaders are far more likely to internalize those costs. When business leaders fully internalize those costs and, therefore, the costs of engaging in risky behavior, they are more incentivized to avoid otherwise marginally profitable relationships with shady third parties. Similarly, they might remain more attuned to third-party risks that develop post-retention to avoid a resulting internal investigation that would significantly reduce or even eliminate their unit's profitability.

Of course, the current economic environment might not be the right time to make these important changes. For example, recommending implementation of a new, robust plan to audit your highest-risk third parties might be all but impossible (or unwise) for the next few months, for a variety of reasons. Changing cost centers to put additional pressure on business units might also be impossible in the current climate. But if you've identified such a needed change, and you have some extra time on your hands, perhaps it might be the time to start to tackle the issue and develop a longer-term strategic plan to get from A to B. Particularly if the current environment exposes such a weakness, documenting the difficulties and building support for the change in the longer term might improve your chances for making the transformation at a later date, when budgets, resources, and business leaders themselves aren't so stressed.

- **Anticipate emergent requests**. Finally, with respect to emergent pressures to circumvent or loosen compliance procedures, it might be worth consulting with legal (or outside counsel) to anticipate such risks and assess which exigent circumstances there may be flexibility for stopgap or alternative measures that balance business necessity and risk mitigation. This topic will be explored further in a subsequent article.

We're here to help

Matthew Queler
Principal
Deloitte Financial Advisory Services LLP
mqueler@deloitte.com
+1 202 744 3223

Ryan Colabello
Senior Manager
Deloitte Financial Advisory Services LLP
rcolabello@deloitte.com
+1 212 436 5104

Ed Rial
Principal
Deloitte Financial Advisory Services LLP
erial@deloitte.com
+1 212 436 5809

Endnotes

1. US Department of Justice Criminal Division, *Evaluation of Corporate Compliance Programs*, April 2019, www.justice.gov/criminal-fraud/page/file/937501/download. ("2019 DOJ Compliance Program Guidance")
2. International Organization for Standardization, *ISO 37001 Anti-Bribery Management Systems*, August 2016, www.iso.org/files/live/sites/isoorg/files/store/en/PUB100396.pdf.
3. 2019 DOJ Compliance Program Guidance at 3 (emphasis added) (citation omitted).
4. *Ibid.*
5. *Ibid.* at 4–5 ("Some companies . . . give employees practical advice or case studies to address real-life scenarios, and/or guidance on how to obtain ethics advice on a case-by-case basis as needs."; "What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)?"; "Have supervisory employees received different or supplementary training?").
6. *Ibid.* at 16 (*quoting* DOJ Corporate Enforcement Policy, Justice Manual § 9-47.120 (2019)); *see also ibid.* at 17 ("Were managers held accountable for misconduct that occurred under their supervision? Did the company consider disciplinary actions for failures in supervision?").
7. *Ibid.* at 6.
8. *Ibid.* at 9.
9. Deloitte, *Forensic Focus on COVID-19: Conducting investigations remotely during times of uncertainty*, April 2020, https://www2.deloitte.com/us/en/pages/advisory/articles/forensic-focus-on-covid-19.html.